COMPUTER AND INTERNET USE POLICY

1 PURPOSE

This Policy sets out the standards of behaviour expected of Persons using AVZ Minerals Limited or any of its subsidiary companies' computer and network facilities.

This Policy is not limited to the workplace or work hours.

2 DEFINITIONS

In this Policy:

"AVZ" refers to AVZ Minerals Limited and all of its associated Subsidiary Companies.

"Confidential Information" includes but is not limited to trade secrets of AVZ; non-public information about the business and affairs of AVZ such as: pricing information such as internal cost and pricing rates, production scheduling software, special supply information; marketing or strategy plans; exclusive supply agreements or arrangements; commercial and business plans; commission structures; contractual arrangements with third parties; tender policies and arrangements; financial information and data; sales and training materials; technical data; schematics; proposals and intentions; designs; policies and procedures documents; concepts not reduced to material form; information which is personal information for the purposes of privacy law; and all other information obtained from AVZ or obtained in the course of working or providing services to AVZ that is by its nature confidential.

"Computer Surveillance" means surveillance by means of software or other equipment that monitors or records information input or output, or other use, of AVZ Computer Network (including, but not limited to, the sending and receipt of emails and the accessing of websites).

"Computer Network" includes all AVZ's internet, email and computer facilities that are used by Users, inside and outside working hours, in the workplace of AVZ (or a related corporation of AVZ) or at any other place while performing work for AVZ (or a related corporation of AVZ). It includes, but is not limited to, desktop computers, laptop computers, tablets, other handheld electronic devices, smart phones and similar products, and any other means of accessing AVZs' email, internet and computer facilities, (including, but not limited to, a personal home computer that has access to AVZs' IT systems).

"Intellectual Property" means all forms of intellectual property rights throughout the world including copyright, patent, design, trademark, trade name, and all Confidential Information including know-how and trade secrets.

"**Person**" includes any natural person, company, partnership, association, trust, business, other organisation or entity of any description, and a Person's legal personal representative(s), successors, assigns or substitutes.

3 USE OF INTERNET, EMAIL AND COMPUTERS

3.1 Appropriate Use

Where use is allowed, users are entitled to use the Computer Network only for legitimate business purposes.

Users are permitted to use the Computer Network for limited and reasonable personal use. Personal use must not impact upon the user's work performance, or AVZ Minerals' resources, or violate this Policy or any other AVZ Minerals policy.

A user must not use the Computer Network for personal use if that use interferes with the efficient business operations of AVZ's or relates to personal business of the user.

AVZ Minerals gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed by any user in the course of using the Computer Network for the User's personal purposes.

3.2 Hardware

Only authorised hardware is permitted to be connected to the Computer Network. Access will not be allowed for any computers, mass storage devices and cameras not issued by the AVZ IT Department (this includes personal computers).

Computers and other IT hardware should be treated with care and respect. Failure of IT hardware resulting from misuse, neglect or wilful damage may result in disciplinary action.

Computers and other IT hardware should not be removed or relocated without authorisation from the IT department. If hardware needs to be relocated, a request should be submitted to the IT department. Portable computers such as laptops and tablets may be temporarily taken off site for work purposes, where required, if approved by a manager and if transported in a suitable bag. To take these units offsite, the unique serial number of the equipment must first be lodged with the security department.

3.3 Data

Users must only access the data and systems that they have been given authorisation to use.

Users must not use computer systems, email or the internet to remove or distribute Confidential Information, or other Company data unless they are authorised to do so.

Users must ensure that all Company data is stored in an appropriate Company data store, such as a network drive, server, intranet, document management system or other suitable

location. Company data should not be stored on the local hard drive of computers as these locations are not backed up.

Users must not delete, destroy, or otherwise degrade Company data unless they are authorised to do so.

Users must not store personal data within company data stores, such as a network drive, server, intranet, document management system and so on.

Any personal data stored on the local hard drive of a computer is stored at the user's own risk, and is subject to the following conditions:

- This data must not include prohibited material as listed in Section 4.1 of this Policy
- This data is not private and may potentially be accessed by the Company during or after the user's term of employment.

3.4 Computer and Account Security

Users must ensure passwords are secure and not shared with other persons. To ensure they are secure, passwords should not be written down or recorded in any other manner that would make them easy for another person to access. This applies to:

- Passwords for AVZ account(s) that provide computer, email or other system access
- Passwords for common resources such as Wi-Fi access.

Users must not use another user's Computer Network facilities (including passwords and usernames/login codes) for any reason without the express permission of the user or AVZ.

To ensure the security of Company data and systems, users must ensure computers are either locked or logged out if they will be left unattended.

Users must not:

- Interfere with or attempt to circumvent remote monitoring and management, anti-virus, firewall or other security tools
- Install software or run unknown or unapproved programs on the Computer Network
- Modify the software or hardware environments on the Computer Network.

If there is a suspected security breach, users should notify the IT department immediately. This includes:

- Unauthorised access to data or systems
- Data loss
- Fraudulent email or other communications
- Hardware or software theft
- Accidental password sharing
- Other activity that could constitute a compromised account.

3.5 Monitoring

AVZ Minerals retains the right to perform Computer Surveillance. This includes but is not limited to:

- Monitoring usage of the Computer Network
- Accessing and viewing all emails sent and received using the email system
- Monitoring access and changes to corporate data.

3.6 Training

If you are not confident with the use of computer systems required for your work, you should notify your manager and request training.

Managers are responsible for ensuring users have the appropriate training to undertake their work.

4 RESTRICTIONS

Users must comply with the following rules when using the Computer Network:

4.1 Restricted Content

Users must not send (or cause to be sent), upload, download, use, retrieve, or access any email or material on the Computer Network that:

- Is obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent in an email or in an attachment to an email or through a link to a site (URL) (e.g. material of a sexual nature, indecent or pornographic material)
- Causes (or could cause) insult, offence, intimidation or humiliation
- May be defamatory or could adversely impact the image or reputation of AVZ Minerals. A defamatory message or material is a message or material that is insulting or lowers the reputation of a Person or group of people
- Involves political debate or opinions or slander
- Is illegal, unlawful or inappropriate
- Affects the performance of, or causes damage to the Computer Network in any way
- Gives the impression of or is representing, giving opinions or making statements on behalf of AVZ without the express authority of AVZ. Further, Users must not transmit or send AVZs documents or emails (in any format) to any external parties or organisations unless expressly authorised to do so.

4.2 Restricted Use

Users shall not use the Computer Network:

- To violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from or into or by using AVZs' computing facilities, except as permitted by law or by contract with the owner of the copyright

- To create any legal or contractual obligations on behalf of AVZ, unless expressly authorised by AVZ
- To disclose any Confidential Information of AVZ or any customer, client or supplier of AVZ, unless expressly authorised by AVZ
- To gain unauthorised access (hacking) into any other computer within AVZ or outside AVZ, or attempt to deprive other users of access to or use of any Computer Network
- To send or cause to be sent chain or SPAM emails in any format
- To use AVZs' computer facilities for personal gain (e.g. running a personal business).

4.3 Restricted Content Blocking

AVZ reserves the right to prevent (or cause to be prevented) the delivery of an email sent to or from a user, or access to an internet website by a User.

4.4 Social Media and Public Website Restrictions

AVZ acknowledges that Users have the right to contribute content to public communications on social media, and other communications platforms and websites not operated by AVZ. Inappropriate use of such communications has the potential to cause damage to AVZ, employees, clients and suppliers. For that reason, the following provisions apply to all Users:

- As it may be possible for any user of an external site to conduct a search that will identify any blogged comments about AVZ, Users must not publish any material that identifies themselves as being associated with AVZ
- Users must not publish any material that may expose AVZ to any possible legal liability (e.g. defamation or discrimination proceedings).

Warning: In addition to potential damaging effects on AVZ, inappropriate content on internal or external platforms and sites can also have adverse consequences for a user in terms of future career prospects, as the material remains widely and permanently accessible to other site users.

5 ENFORCEMENT

Users must comply with the requirements of this Policy. Any breach of this Policy may result in disciplinary action, which may include termination of employment (or, for Persons other than employees, the termination or non-renewal of contractual arrangements).

Other disciplinary action that may be taken includes, but is not limited to, issuing a warning, suspension or disconnection of access to all or part of the Computer Network whether permanently or on a temporary basis.

Document Number: PR000-COR-GO-POL-017

Rev No.	Date	Issued for use	Prepared by	Checked by	Approved by
A	20/02/2020	Draft	MW	MH	